IN THE CLAIMS

Amended claims follow:

1. (Currently Amended) A system for providing dynamic screening of transient messages in a distributed computing environment, comprising:

an antivirus system intercepting an incoming message at a network domain boundary, the incoming message including a header comprising a plurality of address fields storing contents;

a stored set of blocking rules, each blocking rule defining readily-discoverable characteristics indicative of messages infected with at least one of a computer virus, malware and bad content;

a parser module identifying the contents of each address field;

a comparison module checking the contents of each address field against the blocking rules to screen infected messages and identify clean messages;

an intermediate message queue staging each such clean message pending further processing;

an antivirus scanner scanning each message in the intermediate message queue for at least one of a computer virus and malware; and

an event handler performing each scanning operation as an event responsive to each such clean message staged in the intermediate message queue;

wherein the infected messages are blocked from entering the intermediate message queue immediately after the comparison is made between the blocking rules and the contents of at least one of the address fields.

2. (Original) A system according to Claim 1, further comprising:

a message receiver discarding each such infected message without further processing.

3. (Original) A system according to Claim 1, wherein each such blocking rule is specified as a regular expression containing at least one of literal and wildcard values.

4. (Cancelled)

5. (Cancelled)

6. (Original) A system according to Claim 1, further comprising:
a gateway receiving the incoming messages into the network domain boundary.

7. (Original) A system according to Claim 1, wherein the structured fields comprise at least one of sender, recipient, copied recipient, blind copied recipient, date, time, and subject.

8. (Original) A system according to Claim 1, wherein the incoming message comprises at least one attachment.

9. (Original) A system according to Claim 1, wherein the distributed computing environment is TCP/IP-compliant and each incoming message is SMTP-compliant.

10. (Currently Amended) A method for providing dynamic screening of transient messages
in a distributed computing environment, comprising:

intercepting an incoming message at a network domain boundary, the incoming message including a header comprising a plurality of address fields storing contents;

maintaining a set of blocking rules, each blocking rule defining readily-discoverable characteristics indicative of messages infected with at least one of a computer virus, malware and bad content;

identifying and checking the contents of each address field against the blocking rules to screen infected messages and identify clean messages;

staging each such clean message into an intermediate message queue pending further processing;

scanning each message in the intermediate message queue for at least one of a computer virus and malware; and

performing each scanning operation as an event responsive to each such clean message staged in the intermediate message queue;

wherein the infected messages are blocked from entering the intermediate message queue immediately after the comparison is made between the blocking rules and the contents of at least one of the address fields.

11. (Original) A method according to Claim 10, further comprising: discarding each such infected message without, further processing.

12. (Original) A method according to Claim 10, further comprising: specifying each such blocking rule as a regular expression containing at least one of literal and wildcard values.

13. (Cancelled)

14. (Cancelled)

15. (Original) A method according to Claim 10, further comprising: receiving the incoming messages at a gateway into the network domain boundary.

16. (Original) A method according to Claim 10, wherein the structured fields comprise at least one of sender, recipient, copied recipient, blind copied recipient, date, time, and subject.

17. (Original) A method according to Claim 10, wherein the incoming message comprises at least one attachment.

18. (Original) A method according to Claim 10, wherein the distributed computing environment is TCP/IP-compliant and each incoming message is SMTP-compliant.

19. (Previously Presented) A computer-readable storage medium holding code for performing the method according to Claims 10, 11, 12, 15, 16, 17, or 18.

20. (Currently Amended) A system for efficiently detecting computer viruses and malware at a network domain boundary, comprising:

an antivirus system receiving an incoming message packet from a sending client at a network domain boundary through an open connection, the incoming message packet comprising a header including fields, which each store field values, wherein each incoming message packet further comprises a body storing message content;

a message receiver comprising:

a parser module parsing the field values from each field in the header of each incoming message packet by extracting tokens representing the field values;

a comparison module comparing the tokens to characteristics indicative of at least one of a computer virus and malware to identify screened incoming message packets, and forwarding each screened incoming message packet; and

an antivirus scanner scanning the message content of the body of each screened incoming message packet for at least one of a computer virus and malware to identify uninfected screened incoming message packets, and forwarding each uninfected screened incoming message packet;

wherein the screened incoming message packets determined to be infected are blocked from being forwarded immediately after the comparison is made between the tokens and the characteristics indicative of at least one of a computer virus and malware.

21. (Cancelled)

22. (Original) A system according to Claim 20, further comprising:
a message queue enqueueing each screened incoming message packet.

23. (Original) A system according to Claim 20, wherein the antivirus system closes the open connection to the sending client of each non-screened incoming message packet.

24. (Original) A system according to Claim 20, wherein the comparison module analyzes at least one of a sender, recipient, copied recipient, blind copied recipient, date, time, and subject field in the header of each incoming message packet. ,

25. (Original) A system according to Claim 20, wherein the comparison module applies blocking rules to the field values of the header of each incoming message packet.

26. (Currently Amended) A system according to Claim 20, wherein the distributed computing environment is TCP[i]/IP-compliant and each incoming message packet is SMTP-compliant.

27. (Currently Amended) A method for efficiently detecting computer viruses and malware at a network domain boundary, comprising:

receiving an incoming message packet from a sending client at a network domain boundary through an open connection, the incoming message packet comprising a header including fields, which each store field values, wherein each incoming message packet further comprises a body storing message content;

parsing the field values from each field in the header of each incoming message packet by extracting tokens representing the field values;

comparing the tokens to characteristics indicative of at least one of a computer virus and malware to identify screened incoming message packets;

forwarding each screened incoming message packet;

scanning the message content of the body of each screened incoming message packet for at least one of a computer virus and malware to identify uninfected screened incoming message packets; and

forwarding each uninfected screened incoming message packet;

wherein the screened incoming message packets determined to be infected are blocked from being forwarded immediately after the comparison is made between the tokens and the characteristics indicative of at least one of a computer virus and malware.

28. (Cancelled)

29. (Original) A method according to Claim 27, further comprising:

enqueueing each screened incoming message packet onto a message queue.

30. (Original) A method according to Claim 27, further comprising:

closing the open connection to the sending client of each non-screened incoming message packet.

31. (Original) A method according to Claim 27, further comprising:

analyzing at least one of a sender, recipient, copied recipient, blind copied recipient, date, time, and subject field in the header of each incoming message packet.

32. (Original) A method according to Claim 27, further comprising:

applying blocking rules to the field values of the header of each incoming message packet.

33. (Currently Amended) A method according to Claim 27, wherein the distributed computing environment is TCP/[L]IP-compliant and each incoming message packet is SMTP-compliant.

34. (Previously Presented) A computer-readable storage medium holding code for performing the method according to Claims 27,29,30,31,32, or 33.

35. (Previously Presented) The system according to Claim 1, wherein the antivirus scanner scans content of a body of the message and any attachments.

36. (Previously Presented) The system according to Claim 1, wherein the intermediate message queue is maintained at a constant size.

37. (Previously Presented) The system according to Claim 36, wherein the constant size is determined according to a progress of the antivirus scanner in order to prevent the intermediate message queue from becoming overloaded with the messages awaiting scanning.

38. (Cancelled)

39. (Currently Amended) The system according to Claim [38]1, wherein the infected messages are discarded immediately after being blocked from entering the intermediate message queue.

40. (Currently Amended) The system according to Claim [38]1, wherein a connection to a sender of the incoming message is closed if the message is blocked.